

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): M.J. Coss et al.
Case: 1-1-1
Serial No.: 08/927,382
Filing Date: September 12, 1997
Group: 2787
Examiner: Robert Crockett

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Laura M. Hauli Date: July 14, 2000

Title: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

APPEAL BRIEF

Assistant Commissioner for Patents
Washington, D.C. 20231

RECEIVED

JUL 21 2000

GROUP 2700

Sir:

Applicants (hereinafter referred to as "appellants") hereby appeal the final rejection of claims 1-26 of the above-identified application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc., as evidenced by an assignment recorded March 11, 1998 in the U.S. Patent and Trademark Office at Reel 9036, Frame 0268. The assignee Lucent Technologies Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

Claims 1-26 stand finally rejected under 35 U.S.C. §103(a). Claims 1-26 are appealed.

STATUS OF AMENDMENTS

There has been no amendment filed subsequent to the final rejection.

SUMMARY OF INVENTION

The present invention provides techniques for implementing a computer network firewall so as to improve processing efficiency, improve security, and increase access rule flexibility (Specification, page 2, lines 12-14). Particularly, in accordance with claimed aspects of the invention, a computer network firewall is able to support: (a) multiple security policies; (b) multiple users; or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet may be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses (Specification, page 2, lines 14-19).

An illustrative embodiment of the claimed invention is shown and explained in the context of FIGs. 5A, 5B, 6 and 7 of the present application. In particular, FIGs. 5A and 5B illustrate a process for a preferred operation of a firewall processor (e.g., firewall processor 111 in FIG. 1 and/or firewall processor 213 in FIG. 2), including the proper selection of a firewall security policy among a plurality of firewall security policies (Specification, page 5, lines 13-14 and 21-22). The security policies can be represented by sets of access rules which may be represented in tabular form (e.g., as is illustrated in one such table in FIG. 3) and which are loaded into the firewall by a firewall administrator (Specification, page 5, lines 23-24).

In a given firewall implementing an illustrative embodiment of the claimed invention, a decision module or engine, called a "domain support engine" (DSE), determines which security policy to use for a new network session. In this illustrative embodiment, each new session must be approved by the security policies of the source domain and the destination domain(s). The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface (Specification, page 9, lines 11-17).

FIGs. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains according to an illustrative embodiment. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required (Specification, page 9, lines 20-23). In the firewall, each domain is associated with one or more network interfaces.

Interfaces that support more than one domain are separated using an IP address range to distinguish the packets.

Thus, the claimed invention effectively provides a hierarchical rule selection procedure. That is, before a rule is applied to a particular packet, the appropriate set of rules is first selected, and then a rule from the selected set is applied to the packet.

ISSUE PRESENTED FOR REVIEW

Whether claims 1-26 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent No. 5,606,668 (hereinafter "Shwed").

GROUPING OF CLAIMS

The claims of the above-noted group of claims do not stand or fall together. More particularly, claims 1-15 and 17-26 stand or fall together, while claim 16 stands or falls alone.

ARGUMENT

With regard to the issue presented above, the Examiner states in the final Office Action dated December 27, 1999 that claims 1-26 are unpatentable over Shwed. In the final Office Action, the Examiner presents arguments in support of such rejection, attempting to address each of the six independent claims in the present application, i.e., claims 1, 8, 12, 16, 17 and 22, and the respective claims that depend therefrom. Appellants will respectively address below each of the arguments offered by the Examiner with respect to the independent claims, as well as the dependent claims which correspond thereto.

(a) Independent claims 1, 17 and 22

With regard to independent claims 1, 17 and 22, the Examiner states (the final Office Action, page 1, section 2) that "Shwed describes a security system for a computer network that implements packet filtering." Further, the Examiner asserts that "Shwed teaches that his system applies a particular security rule to an incoming packet . . . based on data extracted from the incoming packet." The Examiner goes on to state that, "[a]s per claim 1, Shwed does not explicitly teach that his system derives a session key for the incoming packet. However, processing the extracted packet data in the

Shwed invention . . . would have been recognized by one of ordinary skill in the art, at the time the invention was made, as an obvious equivalent to deriving a session key for the incoming packet.” Lastly, the Examiner states that “Shwed further teaches that a specific TCP destination port may be among data extracted from the incoming packet . . . [and that the Shwed system] is implemented using gateways having multiple network interfaces . . . where the gateway is connected through a router to the Internet.” These arguments appear to constitute the entire basis for supporting the Examiner’s rejection of claims 1, 17 and 22.

The Examiner is apparently ignoring specific claim language in independent claims 1, 17 and 22. More particularly, with regard to claim 1, the Examiner does not address the specific claim language of selecting at least one of a plurality of security policies as a function of the [derived] session key; and using the selected at least one of the security policies in validating said packet. Further, with regard to claims 17 and 22, the Examiner does not address the specific claim language of selecting at least one of a plurality of security policies as a function of the [obtained] data item and using the selected at least one of the security policies in validating packets of the session. Thus, having not expressly stated where in Shwed, or where in the prior art, that such claim limitations are taught or suggested, appellants assert that the rejection is improper. Therefore, appellants assert that claims 1, 17 and 22 are patentable under 35 U.S.C. §103(a) over Shwed.

To the extent that the Examiner intends his comments on page 3 of the final Office Action with regard to claim 8 (to be addressed separately by appellants below) to apply to claims 1, 17 and 22 with respect to selection of a security policy from a plurality of security policies, appellants respectfully assert that such application, even if it were proper to make, still does not teach or suggest the above-mentioned claim language recited in claims 1, 17 and 22.

More particularly, on page 3 of the final Office Action, the Examiner states that “Shwed further teaches . . . that a system administrator may create security rules, and may designate that network objects be separated into sub-groups or domains, where sub-groups may utilize different sets of security rules . . . which would implement multiple sets of security policies.” Appellants respectfully disagree.

Shwed is a system for securing inbound and outbound data packet flow in a computer network by employing security rules in appropriately placed packet filters. Each packet filter may handle multiple security rules, as mentioned at column 4, lines 23-26. The Shwed system identifies

hardware devices controlled by the packet filters as objects. These objects can be grouped depending on their application, e.g., finance department, research and development department, directors of a company protected by the system. Thus, Shwed permits the control of data flow not only to individual devices on its network, but also to groups of devices.

One example of rule selection in accordance with such grouping ability is discussed in Shwed at column 4, line 58-65. There it is explained that, in accordance with the Shwed system, it is possible to have the chief financial officer, as well as other higher ranking officials of the company, be able to communicate directly with the finance group, but filter out communications from other groups. Further, it is possible to allow e-mail from all groups, but to limit other requests for information to a specified set of computers.

This is accomplished by appropriate placement of packet filters and application of a single set of rules within each filter. That is, as explained in Shwed starting at column 7, line 18, a packet is received by a packet filter, compared with a security rule and a determination is made whether or not the packet matches the rule. If the packet matches the rule, a decision may be made to pass or drop the packet based on the requirements of the rule. If the packet doesn't match the rule, then a next rule in the rule set is examined in a similar fashion. Thus, in a manner much like any conventional ordered rule set system, the Shwed system handles group requirements, such as those mentioned in the example above, by simply defining the rules in the single rule set in order to implement the group requirements.

Therefore, rule selection in the Shwed system is significantly different than that provided by the claimed invention. As explained above, the invention provides for first selecting a rule set or security policy from among a plurality of security policies, i.e., rule sets, and then applying a rule from the selected set or policy.

Appellants pointed out this distinction in their Response After Final Rejection filed April 27, 2000. Nonetheless, the Examiner further argues (the final Office Action, page 5, section 3) "applicant fails to disclose in his specification a rule selection procedure distinct from Shwed or not readily known in the art." The Examiner goes on to cite the present application, specifically, page 6, lines 10-11, where it is stated that "[i]n rule processing for a packet, the rules are applied sequentially until a rule is found which is satisfied by the packet" However, reading this portion of the specification in the context of the entire firewall operations described in detail

throughout the present application, one will readily understand that such language cited by the Examiner refers to rule processing for a packet *after* the security policy is selected from among the plurality of policies, i.e., after the applicable rule set is selected, the rules of the selected rule set are applied sequentially until a rule is found which is satisfied by the packet. The support in the present application for security policy selection according to the claimed invention may be found in the various portions of the specification cited above in the “Summary of the Invention” section.

The Examiner further argues (the final Office Action, page 5, section 3) that “rule selection in packet filtering firewall systems at the time the invention was made was routinely based on data fields contained in the packet . . . [and the] applicant’s disclosure does not teach a different rule selection process.” However, as explained above, the claimed invention is directed toward *rule set* selection not just *individual rule* selection.

The Examiner then argues (the final Office Action, page 5, section 3) that “Shwed teaches that his system may be used to create multiple security areas (domains) within a group of networks. It would have been obvious to one of ordinary skill in the art at the time the invention was made that different rules having different packet selection criteria would have applied to different security domains.” The Examiner continues “[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made that the selection of particular rule-based criteria would necessarily be based on data (address fields, control fields, etc.) contained in the packet or on data closely associated with the packet, such as the packet’s hardware interface address.” Again, appellants respectfully disagree. As pointed out above, Shwed only refers to “multiple security rules” (col. 4, lines 24-25) not multiple sets of rules, and handling “groups of computers on the network” is accomplished “by the appropriate placement of packet filters” (col. lines 55-56) not by selecting at least one of a plurality of security policies as a function of the session key (or data item), as expressly recited in claim 1 (and claims 17 and 22). Appellants pointed out these distinctions in their Response After Final Rejection filed April 27, 2000.

Appellants respectfully contend that the hierarchical selection approach of the claimed invention is not obvious in view of Shwed for at least the following reasons. First, the methodology of the invention not only provides for greater rule selection and application flexibility, but also faster overall rule processing for a given packet. Further, independent rule administration is permitted by this methodology, i.e., each rule set may be independently administered, which is a major advantage

over Shwed since Shwed would only permit one administrator to control all packet filter rules associated with the firewall. Also, the present invention permits the downloading, and thus updating of individual rule sets or policies, without affecting other rule sets or policies in the same firewall.

Appellants' attorney conducted a telephone interview with the Examiner on March 27, 2000. During the interview, the Examiner asserted that Shwed refers to rules with "multiple criterion," and that this implies multiple sets of rules. As pointed out in appellants' Response to Office Action dated April 27, 2000, appellants do not specifically see where Shwed refers to rules with "multiple criterion," as mentioned by the Examiner. However, even assuming for argument sake that Shwed does disclose rules with "multiple criterion," this still does not teach or suggest the use of multiple security policies or rule sets according to the invention.

Inasmuch as Shwed and the prior art known to those of ordinary skill in the art at the time of the invention, which the Examiner has characterized as providing certain teachings in the §103(a) rejection of claims 1, 17 and 22, in fact fail to provide those teachings, this §103(a) rejection is believed to be improper and should be withdrawn.

(b) Dependent claims 2-7, 18-21 and 23-26

Appellants hereby re-allege and incorporate by reference the arguments relating to claims 1, 17 and 22 above in their entirety. Due at least to the fact that claims 2-7, 18-21 and 23-26 respectively depend from independent claims 1, 17 and 22, it is believed that such dependent claims are allowable for at least the reasons identified above.

Appellants further note that as to claims 2, 3, 4, 5 19, 21, 24 and 26, the Examiner states (the final Office Action, page 2, section 2) that "Shwed does not explicitly teach that his invention processes all types of Internet protocol packets, such as UDP packets, or all useful packet data, such as IP addresses." However, the Examiner goes on to assert that methods were known "to extract data from headers of TCP packets . . . [as well as UDP packets], and that these methods could have been utilized to extract many types of packet header information, including source address, destination address, next-level protocol, source port, and destination port data." Thus, the Examiner concludes that "[i]t would have been obvious to one of ordinary skill in the art, at the time the invention was made, to program the Shwed invention to process all types of Internet protocol packets and to extract all useful packet header data to assist in security rule decision making, because this would have been

easy to accomplish within the Shwed system” However, regardless of what packet data extraction methods were known at the time the invention was made, no existing firewall system used the extracted data in a security policy selection methodology, as in the claimed invention.

Appellants further note that as to claims 6, 7, 18, 20, 23 and 25, the Examiner states (the final Office Action, page 3, section 2) that “Shwed teaches that his system is implemented using gateways having multiple network interfaces . . . , where the gateway is connected through a router to the Internet.” The Examiner continues that “[g]ateways were well-known to those of ordinary skill in the art, at the time the invention was made, to allow packets to be routed to different network interfaces based on well-known routing algorithms, and that these algorithms could be simply and favorably utilized in conjunction with network security algorithms like those taught by Shwed” Again, whether this is true or not, does not overcome that fact that the Examiner fails to cite any reference or combination of references which teach or suggest utilizing the network interface in a security policy selection methodology, as in the claimed invention.

(c) Independent claims 8 and 12

Appellants hereby re-allege and incorporate by reference the arguments relating to claims 1, 17 and 22 above in their entirety. In addition, with specific regard to independent claims 8 and 12, appellants respectfully assert that the conclusion drawn by the Examiner with respect to Shwed and what the Examiner suggests would have been known to one of ordinary skill in the art at the time of the invention is improper. That is, the rejection is merely conclusory and, in any case, a hindsight application of the reference given the teachings of appellants’ invention.

Claims 8 and 12 provide operations including: designating a plurality of independent security policies, with each of the security policies including a set of access rules, determining which security policy is appropriate for the packet, and validating the packet using the set of access rules of the determined security policy. The Examiner states (the final Office Action, page 3, section 2) that “Shwed does not explicitly teach the use of multiple independent security policies, administered by separate administrators and applied to different groups.” The Examiner further states that “Shwed further teaches . . . that a system administrator may create security rules, and may designate that network objects be separated into sub-groups or domains, where sub-groups may utilize different sets of security rules . . . which would implement multiple sets of security policies,” citing the

portion of Shwed discussed above, i.e., column 4, lines 59-63. The Examiner concludes that “[i]t would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the creation of specific security rules for a particular sub-group of network objects, because this could be accomplished with little modification to the Shwed system, and because the creation of independent security policies by the creation of multiple sets of rules would give users of the Shwed system the benefits of hierarchies of security.”

However, even if appellants agreed with the Examiner’s assertions with regard to the existence of multiple sets of security policies, which appellants do not based at least on the above remarks with respect to claims 1, 17 and 22, there still is no teaching or suggestion of the operations of determining which security policy is appropriate for the packet, and validating the packet using the set of access rules of the determined security policy. As stated above, Shwed does no more than a conventional ordered rule set system in applying a single rule set to a packet wherein the rules of the set are simply defined to effectuate certain actions on a variety of objects. The fact that the objects may be partitioned into groups does not change the fact that only one rule set is used. In other words, in Shwed, all the rules are lumped together into a single set regardless of which object they apply to. There is no suggestion whatsoever to apply a hierarchical rule selection procedure as in the claimed invention. Appellants pointed out this distinction in their Response After Final Rejection filed April 27, 2000.

Inasmuch as Shwed and the prior art known to those of ordinary skill in the art at the time of the invention, which the Examiner has characterized as providing certain teachings in the §103(a) rejection of claims 8 and 12, in fact fail to provide those teachings, this §103(a) rejection is believed to be improper and should be withdrawn.

(d) Dependent claims 9-11 and 13-15

Appellants hereby re-allege and incorporate by reference the arguments relating to claims 8 and 12 above in their entirety. Due at least to the fact that claims 9-11 and 13-15 respectively depend from independent claims 8 and 12, it is believed that such dependent claims are allowable for at least the reasons identified above.

Appellants further note that as to claims 9 and 13, as previously mentioned, Shwed does not provide for corresponding a subset of the security policies to different groups associated with a

single firewall, as recited in claims 9 and 13. Again, Shwed's approach to protecting different groups of computers is not accomplished by having separate rule sets loaded in a single firewall, as in the claimed invention, but rather by appropriate placement of packet filters and application of a single set of rules within each filter (column 4, lines 53-58).

(e) Independent claim 16

With regard to independent claim 16, appellants assert that such claim stands or falls alone, with respect to claims 1-15 and 17-26, and thus is separately patentable for the following reasons. Independent claim 16 recites: segmenting access rules into a plurality of domains; and administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain. These operations are provided in the context of a firewall in a computer network, as recited in the preamble of claim 16. While the claim defines multiple security policies through the segmentation of access rules into a plurality of domains, claim 16 defines the additional inventive concept of administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain. This is neither taught nor suggested in Shwed nor believed to be known to those of ordinary skill in the art at the time of the invention. The invention recited in claim 16 thus provides independent rule administration which is a major advantage over Shwed since Shwed would only permit one administrator to control all packet filter rules associated with the firewall.

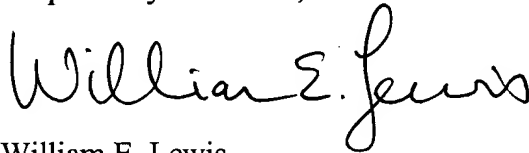
The Examiner contends (the final Office Action, page 4, section 2) that "although Shwed does not explicitly teach that only the administrator of a domain is allowed to modify the security policy rules for that domain, it would have been obvious to one of ordinary skill in the art, at the time the invention was made, to restrict the creation of security rules for a particular sub-group of network objects to a particular system administrator, because this could be accomplished with little, if any, modification to the Shwed system, and because the creation of rules by a specialist in a particular domain would give the benefits of increased security and confidence in the Shwed system."

Appellants respectfully contend this is merely conclusory and, in any case, a hindsight application of the reference using the teachings of appellants' invention. Thus, even if Shwed could be so modified, the fact that one could modify something does not necessarily make it obvious or desirable to do so. Without any suggestion to do so, or in the face of teaching away from doing so,

as in the case of Shwed, such possible modification is not obvious. As stated above, Shwed's approach to protecting different groups of computers is not accomplished by having separate rule sets loaded in a single firewall, as in the claimed invention, but rather by appropriate placement of packet filters and application of a single set of rules within each filter (column 4, lines 53-58). This only suggests, and appellants suggest necessitates, a single administrator for the entire single rule set. Appellants pointed out this distinction in their Response After Final Rejection filed April 27, 2000. Thus, since there is no suggestion to include multiple security policies in a single firewall device, there can be no suggestion to provide independent administration of respective security policies in a single firewall device, as in the claimed invention.

Inasmuch as Shwed and the prior art known to those of ordinary skill in the art at the time of the invention, which the Examiner has characterized as providing certain teachings in the §103(a) rejection of claim 16, in fact fail to provide those teachings, this §103(a) rejection is believed to be improper and should be withdrawn.

Respectfully submitted,

A handwritten signature in cursive script that reads "William E. Lewis".

Date: July 14, 2000

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

APPENDIX

1. A method for validating a packet in a computer network, comprising the steps of:
 deriving a session key for said packet;
 selecting at least one of a plurality of security policies as a function of the session key; and
 using the selected at least one of the security policies in validating said packet.
2. The method of claim 1 wherein the session key includes items derived from header information appended to data in said packet.
3. The method of claim 1 wherein the session key includes at least one item from the set consisting of (i) a source address, (ii) a destination address, (iii) a next-level protocol, (iv) a source port associated with a protocol, and (v) a destination port associated with the protocol.
4. The method of claim 1 wherein the session key includes at least one item from the set consisting of (i) an Internet protocol (IP) source address, (ii) an IP destination address, (iii) a next-level protocol, (iv) the source port associated with the protocol, and (v) the destination port associated with the protocol.
5. The method of claim 3 wherein the next-level protocol is transmission control protocol (TCP) or universal datagram protocol (UDP).
6. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface at which the request was received.
7. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface to which the request is to be sent.

8. A method for validating a packet in a computer network, comprising the steps of:
designating a plurality of independent security policies, with each of the security policies including a set of access rules;
determining which security policy is appropriate for the packet; and
validating the packet using the set of access rules of the determined security policy.

9. The method of claim 8 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

10. The method of claim 8 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

11. The method of claim 8 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

12. An apparatus for use in validating a packet in a firewall of a computer network, the firewall designating a plurality of independent security policies, with each of the security policies including a set of access rules, the apparatus comprising:

a processor associated with the firewall and operative (i) to process the packet to determine which of the security policies is appropriate for the packet, and (ii) to validate the packet using the set of access rules of the determined security policy.

13. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

14. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

15. The apparatus of claim 12 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

16. A method of providing a firewall in a computer network, comprising the steps of:
segmenting access rules into a plurality of domains; and
administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

17. A computer system for packet validation in a computer network, comprising:
means for obtaining at least one data item from a request for a session;
means for selecting at least one of a plurality of security policies as a function of the data item; and
means for using the selected at least one of the security policies in validating packets of the session.

18. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface at which the request was received.

19. The computer system of claim 18 wherein the means for determining comprises means for referring to a source IP address contained in the request.

20. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface to which the request is to be sent.

21. The computer system of claim 20 wherein the means for determining comprises means for referring to a destination IP address contained in the request.

22. A method for packet validation in a computer network, comprising the steps of:
obtaining at least one data item from a request for a session;
selecting at least one of a plurality of security policies as a function of the data item;
and

using the selected at least one of the security policies in validating packets of the session.

23. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface at which the request was received.

24. The method of claim 23 wherein the determining step includes referring to a source IP address contained in the request.

25. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface to which the request is to be sent.

26. The method of claim 25 wherein the determining step includes referring to a destination IP address contained in the request.